6. tétel **Access Lists** (Hozzáférési listák)

I’m a network system engineer of a company which produces routers. I was asked to perform a professional presentation about Access-lists at beginner’s level to the traders of retailers. (viszonteladók kereskedőinek).

The Internet is wide open, operating with a low level of security. There are millions of users and security has become very important. Companies secure their networks to prevent uncontrolled or unasked access to their private networks from the outside. From security consideration (biztonsági megfontolásból) it is very important to apply access lists. Most network designers use firewall to protect the security of the network and from the unauthorized users.

An access list regulates (szabályozza) the traffic to permit or deny packets. It limits the network traffic in order to increase the capacity (növelje a teljesítményt). It filters the traffic, permits or denies if it is an e-mail or Telnet. It also permits or denies accessing the network services for the hosts. We can also configure a simple firewall on a Cisco router. The rules of Access Control Lists (ACL) ensure the basic network traffic filtering. Cisco routers use ACLs to permit or deny the network traffic. ACLs are powerful tools to control inbound and outbound network traffic. They can be assigned to all managed protocols, e.g. IP, IPv6 or IPx. The main reason for using ACLs is to build a secure network.

In data segment, a port number can be found which identifies the application. The access list reads the following information: the source address, the destination address and the protocol type.

You can have problems with access lists. One of the most common problems associated with access list is a lack of planning (tervezés hiánya). Another problematic area is the sequential nature (egymás utáni jelleg) in which you must enter the list into the router. Many new network administrators find themselves in trouble when they Telnet into a router and begin applying an access list.

There are some important rules to access lists. At first you have to create the access list then you can apply to interfaces. The access lists can be applied to inbound or outbound traffic. Inbound means direction is into the router. Outbound means direction is out of the router. Inbound ACLs are good for packet filtering when you have to examine the only source address to the packets arriving at inbound interface. Outbound ACL is good if you apply the same filter to more several inbound packets but also the outbound packets on the same interface.

There are some other access list rules. Routers apply lists sequentially in the order (olyan sorrendben) in which you type them into the router. Routers apply lists to packets sequentially (egymás után). Packets are processed only until a match (egyezés) is made and then they are acted upon based on the access list criteria contained in access list statements. Implicit deny means that anything blocks all packets that do not meet requirements (követelmény) of the access lists unless (hacsak nem) permit any command is used at the end of the list. Implicit deny doesn’t permit any traffic, that’s why in ACLs you need at least one permitting command or else all traffic gets to blocking.

Access lists must be applied to an interface as either (vagy) inbound or (vagy) outbound traffic filters. Only one list, per protocol, per direction can be applied to an interface. You cannot remove one line from an access list. Access list are effective as soon as they are applied.

All in all, companies need access lists in order that (azért, hogy) uninitiated (jogosulatlan) people can’t damage websites.